

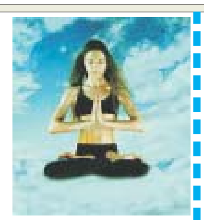


PERIODICO DE NETWORKING

n°6
MARZO 2004

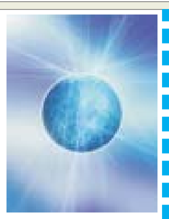
VMWare

Una máquina virtual es una aplicación que permite emular varias otras máquinas dentro de una misma. ¿Cómo es esto?



Elementos de Criptografía

Continuamos en este artículo con el tema desarrollado en la anterior edición de NEX



Windows Server 2003

Las nuevas características introducidas por Microsoft a su nuevo sistema operativo Windows Server 2003










Marzo 2004.

Seguimos recibiendo vuestros comentarios positivos respecto de NEX y de nuestros artículos, en particular con la inaguración del suplemento de Seguridad Informática.

En este número abrimos una nueva sección: Laboratorios NEX. En ella detallaremos mes a mes productos que probamos exhaustivamente en nuestros laboratorios. OVIS Link, Taiwan nos ha provisto en esta oportunidad de sus productos wireless. Para su mejor apreciación en la misma sección detallaremos las tecnologías utilizadas por tales dispositivos.

En este número presentaremos un artículo muy detallado de TCP/IP. Saber cómo se confroman los paquetes TCP/IP es indispensable para entender seguridad informática.

Windows Server 2003 ha hecho su debut hace pocos meses y aquí mostramos sus diferencias con Windows 2000.

Y no se pierdan el artícuo de O'Reilly, una de las editoriales más prestigiosas del mundo de IT.

Nuevamente invitamos a aquellos interesados en colaborar con artículos o que quieran hacernos llegar sus comentarios, a enviarlos a articulos@nexweb.com.ar



Staff

Año 3 Nº 5 2004

Director
Dr. Osvaldo Rodríguez

Propietarios
COR Technologies S.R.L.

Coordinador Editorial
Carlos Rodríguez Bontempi

Cordinación General
María Lujan Zito

Responsable de Contenidos
Dr. Osvaldo Rodríguez

Editor en Jefe
Raúl Kuzner

Redactores
Martin Sturm, Javier Pierini, Raúl Kuzner, Osvaldo Rodriguez, Maria Lujan Zito, Hugo Cela, Leonel F. Becchio, Rodrigo M. Gonzalez.

Humor
Marcos Severi

Distribución
Lorena De Lillo, Ximena Antona

Diseño Web SIte
Emanuel A. Rincón

Diseño Gráfico
Carlos Rodríguez Bontempi

Publicidad
Ximena Antona
publicidad@nexweb.com.ar
4312-7694

Preimpresión e Impresión
Edigráfica S.A. Tel:4846236

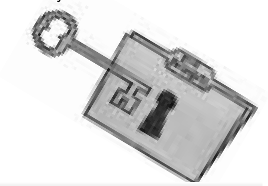
Periódico de Networking
Registro de la propiedad Intelectual en trámite leg3038

Dirección: Córdoba 657 12°Capital Federal
Tel:(011) 4312-7694 http:// www.nexweb.com.ar

El staff de Nex colabora ad-honoren, si desea escribir para nosotros enviar un e-mail a: articulos@nexweb.com.ar

Retire su ejemplar NEX en forma gratuita en Córdoba 657 piso 12° Capital Federal o solicítelo telefónicamente para su empresa al (011) 4312-7694 http:// www.nexweb.com.ar



Entendiendo TCP/IP

(Los fundamentos para comprender seguridad informática)



Toda la información que viaja por Internet (y en redes en general) está contenida en "frames" (paquetes). Estos paquetes están conformados por los "datos" que una cierta aplicación quiere enviar (por ejemplo envío: "dominio *yahoo.com* dame tu página web" al hacer *http://www.yahoo.com*). A éstos "datos" se le adicionan "headers" (encabezados) por los diferentes protocolos de TCP/IP. Lo malo, lo bueno, lo que quiere hacer mal, todo está dentro de los "frames".

TCP/IP es una suite (conjunto) de protocolos. Como ya dijimos, cada protocolo en un dado orden, agrega a los "datos" a ser enviados un "header". Allí se incluye la información del número IP del que envía, del que recibe, el puerto de la aplicación que envía los datos, el puerto destino y toda otra información relevante a la comunicación.

Quienes quieran realizar una maldad (hackers) o quienes desarrollen herramientas de protección (antivirus, firewalls, proxys) deberán conocer a fondo el detalle de cómo están conformados los paquetes.

En este artículo se explicará ese detalle. Se verá una introducción histórica de TCP/IP, el modelo que lo describe, y un análisis de los headers que se agregan cuando se conforman los paquetes.

Si desea entender cualquier artículo sobre seguridad o implementar alguna herramienta será indispensable tener claro lo aquí expuesto. En NEX 7 se explicitará un detalle ampliado sobre los protocolos IP, TCP y UDP.

TCP/IP

Los protocolos TCP/IP (también llamados "Internet Protocols") son la "amalgama" que conecta hoy la mayoría de las redes de computadoras. También son responsables de la existencia de Internet: la red de redes que nos permiten entre otras cosas enviar correo electrónico, poder ver páginas Web y realizar transacciones comerciales en materia de segundos sin tener un límite geográfico. Los protocolos TCP/IP fueron originalmente desarrollados para soportar tareas de investigación pero han logrado un alto grado de maduración y aceptación casi universal. Las investigaciones realizadas por el mundo académico fue financiado en su mayor parte con subsidios de las fuerzas armadas americanas, a través del proyecto ARPANET (Advanced Research Project for Networking. Año 1969).

En 1983 se divide en dos redes MILNET (de uso militar) e INTERNET (de uso académico). En 1990 INTERNET se hace comercial y surge el boom del e-commerce e infinidad de otros mundos.

TCP/IP se refiere a un conjunto (suite) de protocolos para comunicación de datos. La suite toma su nombre de dos de los protocolos que lo conforman: Transmition Control Protocol (TCP) e Internet Protocol (IP). La figura 1 nos detalla algunos de los protocolos más comunes que conforman la suite.

Modelos para describir la arquitectura de comunicación de datos

Un modelo arquitectónico fue desarrollado por la International Standards Organization (ISO) y usado para describir la estructura y función de los protocolos de comunicación de datos: OSI (Open Systems Interconnect Referente Model). Ver Figura 2.

Contiene siete capas (layers) que definen las funciones de los protocolos de comunicación de datos. TCP/IP puede ser descrito con el modelo OSI pero existe un modelo de arquitectura (alternativo) propio (ver figura 2, TCP/IP implementación) compuesto por cuatro capas.

Cada capa representa una función que se realiza en la transferencia de datos entre aplicaciones a través de la red. Se lo llama un "apilamiento" o "stack".

Una capa no define un solo protocolo. Define una función que puede ser realizada por un número de protocolos. Por ejemplo, un protocolo de transferencia de archivos (FTP) y una de correo electrónico (SMTP) proveen servicios al usuario y son parte del Application layer.

Cuando dos máquinas se comunican, cada protocolo se comunica con su "peer" (par). Un par es una implementación del mismo protocolo en la capa equivalente en el sistema remoto.

En principio cada protocolo debería solo interesarse de la comunicación con su peer. Sin embargo, deberá también haber un acuerdo de cómo pasar los datos entre capas dentro de una sola computadora. Los datos son pasados bajando por el "stack" de una capa a la otra hasta que es transmitida por los protocolos de la llamada "Physical Layer" por la red. Por otro lado los datos son tomados de la red y subidos a través del "stack" hasta la aplicación receptora.

Las capas individuales no necesitan saber como funcionan la capa superior e inferior a ella: solo como pasar los datos. (ver fig. 3)

Este aislamiento de funciones en cada capa minimiza el impacto sobre toda la suite, que se pueden producir por los avances tecnológicos. En cada capa del "stack" se adiciona información de control llamado "header" (encabezado) ya que se coloca al frente de los datos a transmitir (ver fig. 4)

Cada capa trata toda la información que recibe de las capas superiores como "datos" y adiciona "su" propio "header" (proceso llamado encapsulación). Cuando se recibe información sucede lo opuesto.

Es importante resaltar que cada capa define una estructura de datos independiente de las otras y su propia terminología que la describe. La figura 5 muestra los términos usados en las diferentes capas para referirse a los datos transmitidos (i.e un "datagram" tiene el "header" correspondiente a la internet layer y lo que le pasa la capa superior).

Descripción de cada layer (capa)

Las figuras 6,7 y 8 muestran una representación pictórica de la estructura de los "headers" y datos. Los "headers" están conformados por varios "words" de 32 bits donde se incluye información. Recordar que cada layer tiene su propia estructura (Fig. 4.) y agrega un "header" a lo que recibe de la capa superior que lo toma como "datos". Esta información adicional que garantiza el "delivery"(entrega) se llama "encapsulación". Cuando se reciben "datos" lo opuesto sucede.

TCP/IP Suite — Figura nro. 1

Los protocolos asociados con TCP/IP incluyen los siguientes:

IP	Internet Protocol
TCP	Transmission Control Protocol
IGMP	Internet Group Management Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
RARP	Reverse Address Resolution Protocol
UDP	User Datagram Protocol
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

Arquitectura TCP/IP — Figura nro. 2

Modelo OSI	Implementación TCP/IP
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Interface Layer
Physical Layer	

Cada layer elimina su "header" antes de pasar los "datos" a la capa superior. Cuando la información sube el stack, lo que llega de la capa inferior es interpretada como header y datos.
La información de los estándares de los diferentes protocolos es desarrollada y publicada a través de los llamados "Request For Comments". (Ver nota)

NETWORK ACCESS LAYER (Capa de Acceso a la red)

La Network Acess Layer es la de más abajo en la jerarquía de protocolos TCP/IP. Los protocolos en está capa proveen el modo en que el sistema envía los datos a otros dispositivos en una red a la que esta directamente conectado.
Si aparecen nuevas tecnologías de hardware deberán desarrollarse nuevos protocolos para la Network Access Layer. Hay muchos protocolos de acceso: uno para cada Standard de red física. (Ethernet, Token Ring, Cobre-teléfono, Fibra.)
Las funciones que se realizan a este nivel incluyen encapsulación de datagramas IP: ("frames" que se transmiten por la red) y el mapeo de números IP a las direcciones físicas usadas por la red (i.e el MAC address)

Dos ejemplos de RFCs que definen protocolos de esta capa son:
RFC 826 ARP (Address Resolution Protocol) resuelve numeros IP a MAC addressses.
RFC 894 especifica como se encapsulan los datagramas para transmitirlos por las redes Ethernet.

Internet Layer.
Esta es la capa arriba de la Network Access Layer. El "Internet Protocol"(IP) es el corazón de TCP/IP y el protocolo más importante de esta layer. Todos los protocolos en capas superiores e inferiores lo usan para "el delivery" de datos. IP está complementado por ICMP (Internet Control Message Protocol).

IP (Internet Protocol)
IP es el protocolo sobre el que se basa Internet. IP es un protocolo connectionless. (Ver nota). Además se basa en protocolos de otras layers para realizar "error detection y recovery".
Sus funciones incluyen: definición de "datagrama" (la unidad básica de transmisión en Internet); definición del esquema de addressing (números IP y como funcionan); definir como mover datos entre la Network Accesss Layer y la Transport Layer; como se rutean "datagramas" a hosts remotos; como realiza fragmentacion y re-armado de "datagramas".
La figura 6 nos muestra un esquema del datagrama IP.
Recomendamos estudiar este esquema. En NEX 7 veremos el detalle de cómo se utiliza toda la información en el header.

ICMP (Internet Control Message Protocol). Protocolo de Control de Mensajes de Internet.
Es complementario al Internet Protocol y fue definido por el RFC 792. Forma parte de la Internet Layer. Manda mensajes realizando tareas de control como reporte de errores e información de funcionamiento de TCP/IP

Algunos ejemplos de sus funcionalidades: Control de flujo: Si los datagramas llegan muy rápido para ser procesados, el host que los recibe o un gateway (router) en el camino, manda el llamado ICMP "Source Quench Message" a quien envió el mensaje. Este detiene temporariamente los envíos. Destinos no accesibles:(Unreachable). Si un sistema se da cuenta que el destino de un paquete es no accesible envía a la fuente (source) un "Destination Unreachable Message". Si el destino no accesible es un host o network, el mensaje lo envía un gateway (router) intermedio. Pero si el destino es un "puerto" no accesible, el host destino envía el mensaje. Redireccionamiento de ruta: Si un gateway (router) se da cuenta que otro gateway es una mejor opción, le envía al host fuente un "ICMP Redirect Message". Chequeo de hosts remotos. Un host puede querer saber si otro host está operando. Envía un ICMP "Echo Message". Cuando el segundo host recibe el echo message, contesta re- enviando el mismo paquete. El comando "ping" usa este mensaje.

La Tabla 1 muestra los códigos que son utilizados por ICMP para los ejemplos anteriores y otros casos.

Figura nro. 3

Una conversación TCP/IP

HTTP — Logical
Application Layer
Transport Layer
Internet Layer
Network Interface Layer

1. El layer de aplicación prepara un pedido HTTP.
2. TCP negocia el envío garantizado de los datos. Un header TCP es agregado al pedido en esta layer.
3. El header IP, incluyendo la dirección IP de las computadoras remitente y destinataria, es agregado al paquete.
4. Las direcciones físicas para computadoras que envían y reciben son agregadas al paquete. La información es transmitida como señales de luz o electricidad a la otra computadora.
5. Cuando el paquete llega a la otra computadora, va en sentido reverso a traves de layers.
6. El servidor de Web , envía los datos solicitados utilizando el mismo proceso.

Figura nro. 4

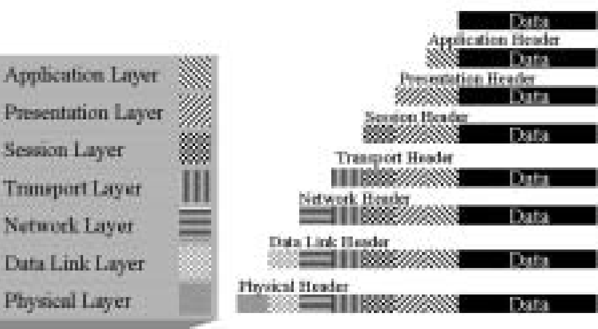


Tabla nro. 1

Tipo de código	Mensaje ICMP
0	Respuesta a eco (respuesta a PING)
3	Destino inaccesible
4	Source query
5	Redirección
8	Eco (petición de PING)
11	Tiempo de vida excedido (TTL)
12	Problema en algún parámetro
13	Petición de marca de tiempo
14	Respuesta de marca de tiempo
17	Petición de máscara de red
18	Respuesta de máscara de red

Figura nro. 5

Layer	TCP	UDP
Application Layer	Stream	Message
Transport Layer	Segment	Packet
Internet Layer	Datagram	Datagram
Network Access Layer	Frame	frame

Protocolos
Cuando las computadoras se comunican, es necesario definir un conjunto de reglas que gobiernen su comunicación. Este conjunto de reglas se llaman protocolos.
Los protocolos TCP/IP están disponibles para cualquiera, desarrollados y cambiados por consenso. Y, han sido adoptados universalmente, lo que permite la conectividad de redes heterogéneas.

TRANSPORT LAYER

Los dos protocolos más importantes en esta capa son TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). TCP nos provee un servicio de entrega de datos confiable. Incluye detección y corrección de errores end-to-end (de punta a punta). UDP provee un servicio de entrega "connectionless" y mucho más reducido. Ambos, además, mueven los datos entre los Application layer e Internet layer dentro de la misma máquina. Quien programe una aplicación dada elegirá qué servicio es el más apropiado.

UDP (User Datagram Protocol)

UDP es un protocolo "connectionless" y no-confiable (no-confiable significando que no existe dentro del protocolo una infraestructura que cerifique que los datos llegan al destino correctamente). El header UDP (ver figura 7) utiliza en la "word1" 16 bits para detallar el Source-Port (puerto fuente) y otros 16 para el Destination-Port (puerto destino). De este modo sabe (por el número de puerto) qué aplicación lo envió y cuál lo recibirá.

¿Porqué decide quien programa una aplicación usar UDP?. Puede haber varias razones. Por ejemplo, si la cantidad de datos es muy pequeña, el overhead de crear la conexión y asegurarse la entrega puede ser mayor que re-transmitir los datos. Aplicaciones del tipo pregunta-respuesta son excelentes candidatos.

La respuesta misma se puede usar como un aviso positivo de entrega. Si no llega una respuesta en un dado tiempo la aplicación vuelve a enviar su pedido. Puede también ser que una dada aplicación provea su propia infraestructura para entrega confiable y no necesitara una infraestructura más compleja que UDP.
Ver Fig. 7

TCP (Transmission Control Protocol) (Procolo de Control de Transmisión)

Las aplicaciones que necesiten que se les provea de una infraestructura confiable usarán TCP. Usando TCP estará segura de que los datos llegaron a destino y en la secuencia adecuada. TCP es un protocolo confiable, "connection-oriented" y "byte-stream".

En NEX 7 ampliaremos detalles de TCP. Un estudio de la figura 7 nos indica qué información utiliza para establecer lo que se llama el "three way handshake" (estrechado de mano de tres pasos). En el word1 (al igual que en UDP) se envia la información de los puertos origen y destino. Pero en este caso es enviada mucha más información.

APPLICATION LAYER

PROTOCOLOS DE CAPA DE APLICACIÓN

En la capa superior de la arquitectura TCP/IP está la Application Layer. Esta incluye todos los procesos que utilizan a la Transport Layer como medio de entrega de datos.
Es la parte de TCP/IP donde se procesan los pedidos de "datos" o servicios. Las aplicaciones de esta capa están también esperando pedidos para procesar y están "escuchando" por sus puertos respectivos.

La Application Layer NO es donde está corriendo un procesador de palabras (por ejemplo WORD), una hoja de cálculo o un browser de Internet (Netscape o Internet Explorer). Las aplicaciones que corren en esta capa, SI, interactúan con los procesadores de texto, programas de hoja de cálculo y otras.

Figura nro. 6

Versión IP (4 bits)	Longitud de la cabecera (4 bits)	Tipo de servicio (8 bits)	Longitud total (16 bits)				
Identificación (ID) del fragmento (16 bits)			R	D F	M F	Posición de fragmento (13 bits)	
Tiempo de vida (TTL) (8 bits)		Protocolo (8 bits)	Suma de comprobación de la cabecera (16 bits)				
Dirección IP de origen (32 bits)							
Dirección IP de destino (32 bits)							
Opciones (longitud variable que se completa con ceros hasta 40 bits)							
Datos							

Figura nro. 7

Número de puerto de origen (16 bits)	Número de puerto de destino (16 bits)
Longitud (16 bits)	Suma de comprobación (16 bits)
Datos	

Figura nro. 8

Número de puerto de origen (16 bits)								Número de puerto de destino (16 bits)
Número de secuencia (32 bits)								
Número de acuse de recibo (32 bits)								
Desplazamiento (4 bits)	Reservado (6 bits)	U	A	P	R	S	F	Ventana (16 bits)
Suma de comprobación (16 bits)								Puntero urgente (16 bits)
Opciones (Longitud variable y relleno con ceros)								
Datos								

Figura nro. 9

Combinación de indicadores	Significado
SYN	Primer paquete de la conexión que especifica el pedido de comunicación con el equipo destino.
SYN/ACK	El segundo equipo responde y envía su SYN.
ACK	En cada envío se activa este bit para asegurar que el envío anterior se ha recibido correctamente.
FIN	Señal enviada por el equipo que está preparado para cerrar la conexión.
FIN/ACK	Señal enviada por el segundo equipo para aceptar el cierre de conexión y validar el estado de recepción de paquetes.
RST	El paquete RST se envía para dar aviso de recepción de paquetes no esperados. Un caso claro es el de un paquete SYN/ACK que llega sin haber recibido previamente un paquete SYN.

Los protocolos SMTP, http, Telnet, POP, DNS o FTP son ejemplos de protocolos de esta layer.

Request For Comment (RFC).

La naturaleza abierta de los protocolos TCP/IP requiere documentación pública de los estándares. La mayor parte de la información de TCP/IP se publica como Request for Comments (RFC). Como implica el nombre, el estilo y contenido de estos documentos es poco rígido. Los RFC contienen información bastante completa y no se remiten solamente a las especificaciones formales.

Protocolos Connection oriented y Protocolos connectionless (no orientado a connección)

Protocolo connection oriented: intercambia información de control con el sistema remoto (llamada handshake (dado de mano), para verificar que está listo para recibir datos antes de enviarlos.
Se establece una "connection" end-to-end.

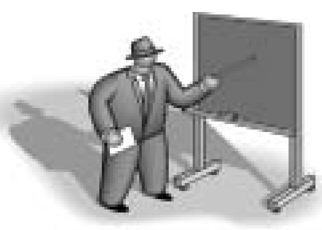
(Ejemplos TCP)
Protocolo connectionless: Que NO intercambia información de control.

¿Porque triunfó TCP/IP sobre otras alternativas?

Son protocolos abiertos, disponibles gratuitamente y desarrollados en forma independiente de cualquier vendor de hardware o sistema operativo. Son independientes de cualquier hardware físico particular. TCP/IP puede correr sobre Ethernet, Token Ring, línea telefónica dial-up, X.25 net y virtualmente cualquier otro tipo de medio físico de transmisión. Un esquema de "addressing" (direccionamiento) universal que permite a cualquier dispositivo TCP/IP dirigirse en forma única a cualquier otro dispositivo de la red aún cuando la red sea tan grande como el world-wide Internet.

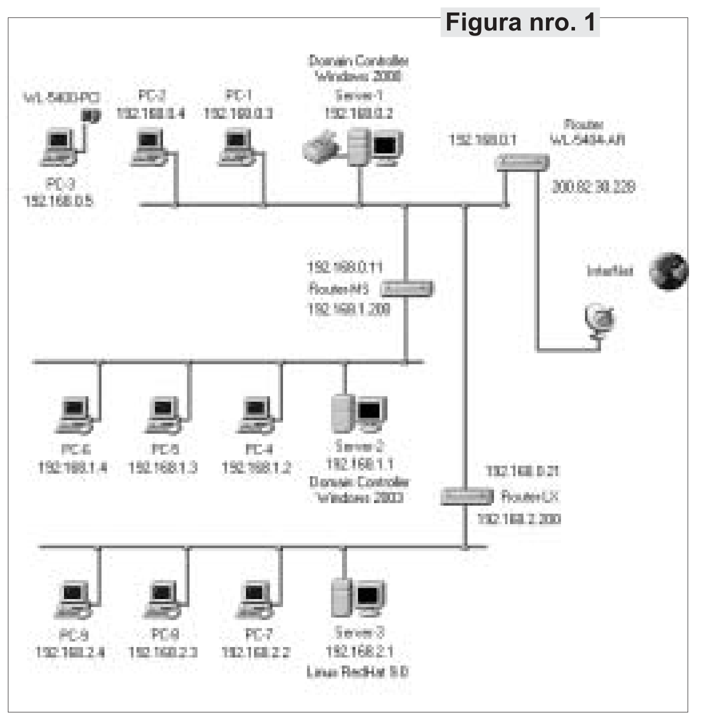
NEX - LAB - NEX - LAB

LABORATORIO



Inauguramos una nueva sección: Laboratorios NEX. Aquí analizamos productos de diferentes vendors realizando un análisis crítico de sus funcionalidades y características más importantes. En este numero Ovis Link-Taiwan (www.ovislink.com.tw) nos ha provisto de una infraestructura wireless para probar en nuestros laboratorios.

Figura nro. 1



Wireless LAN (LAN inalámbrica) conectada a InterNet

Recomendamos como material suplementario leer 2 artículos anteriores de NEX a modo de introducción: seguridad en entornos inalámbricos y el ABC de redes inalámbricas que fueron publicados en NEX2 (ver *www.nexweb.com.ar*)

Hemos recibido 3 productos de OvisLink-Taiwan (*www.ovislink.com.tw*) necesarios para crear una LAN wireless:

1. WL-5404AR. Router, WireLess Access Point y 4 bocas Switch 10/100 Mbps (ver nota).
2. WL-5400PCI. Placa de Red PCI con Conectividad WireLess (ver nota).
3. GSH8T Gigabit Switch de 8 bocas (ver nota). Este switch será evaluado en detalle en NEX 7.

Las pruebas de Laboratorio las hemos realizado sobre los dos productos wireless (WL) integrándolas en la red de la figura 1:

Las prestaciones han sido excelentes y muy cerca de los valores descriptos en los manuales. El WL-5404AR permite configurar todas las prestaciones vía HTTP, simplemente apuntando el navegador Web a la dirección IP asignada al Router.

Ovislink ha incluido aquí un firewall que incluye entre otras características SPI (*Stateful Packet Inspection*-Inspección Completa de Paquetes), detección de ataques DoS (*Denial of Service*-Denegación de Servicio) (ver más detalles en la nota).

Vía e-mail el administrador recibe un reporte de posibles ataques. El filtro de contenido y el ACL (*Access Control List*-Lista de Control de Acceso) le dan a quien administra, posibilidad de monitorear y controlar la red con resultados de prestaciones y seguridad óptimos.

Switch vs Hub

Un Hub es simplemente un repetidor de paquetes. Cada vez que un paquete, proveniente de cualquiera de los puertos, llega al Hub, éste simplemente lo distribuye a todos los demás puertos. Las únicas verificaciones que hace son exactamente las mismas que se hacen cuando la red entre las maquinas es un simple cable coaxil: CSMA/CD (*Carrier Sense Multiple Access/Collition Detection*-Acceso Múltiple con Detección de Portadora y Colisiones). Por esta razón es considerado un dispositivo de Capa 1 (Modelo OSI).

Un Switch en cambio, aprende las MAC Address que hay en cada puerto y cuando hay tráfico proveniente de un puerto, inspecciona el encabezado del paquete para obtener la MAC Address de destino y entonces solamente lo envía en el puerto que corresponde. Por esta razón es considerado un dispositivo de Capa 2 (Modelo OSI).

Esta manera de distribuir los paquetes mejora notablemente la performance de la Red.





NEX - LAB

Placa PCI Wireless WL-5400-PCI

Prestaciones y Compatibilidad

La WL-5400-PCI es una placa de red inalámbrica PCI de altas prestaciones para PC's. Compatibilidad total con el último estándar IEEE 802.11g y opera en el mismo espectro de frecuencias que el 802.11b. La potencia de emisión es de 17 dBm obteniendo así, tanto prestaciones como velocidad y distancia de alcance. Esta placa por lo tanto es compatible con la mayoría de dispositivos 802.11b y 802.11g. Está equipada con una antena desmontable (incluida) que permite futuras mejoras usando antenas de mayores ganancias.

Mayor Seguridad

OvisLink ha incorporado los últimos sistemas de seguridad. El estándar de encriptación WPA (Wi-Fi Protected Access) se ha desarrollado para fortalecer la seguridad en las transmisiones wireless. La clave del WPA está en el uso de TKIP (*Temporal Key Integrity Protocol*-Protocolo de Integridad de Claves Temporales) para reforzar la encriptación de los paquetes wireless. TKIP incluye funciones de seguridad como; función de mezcla de claves por paquete, MIC (*Message Integrity Check*-Chequeo de Integridad de Mensaje), IV (*Initialization Vector*-Vector de Inicialización) y mecanismo de cambio de claves. Con todas estas funciones se elimina la vulnerabilidad de la simple encriptación WEP. La encriptación WEP también está incorporada, en 64 y 128 bits.

¿Qué es NAT?

Un Router que comparte internet, también conocido como un "*NAT Router*", usa una técnica llamada Traducción de Dirección de Red (*Network Address Translation*-NAT) para permitir a una red compartir una única dirección IP. Para poder realizar esta tarea, NAT antepone al número de puerto un valor para poder reconocer los datos de diferentes máquinas.

En la red que está conectada detrás de un Router NAT, normalmente se asignan direcciones IP privadas (p.ej.: **192.168.0.4**). Cuando la computadora **A** envía un paquete (digamos que usa el puerto **1024**), dentro de la información del encabezado del paquete estará la siguiente información: **192.168.0.4:1024**; cuando este paquete alcanza el Router para seguir hacia la red externa, el Router simplemente agrega un prefijo (digamos **30**) al número de puerto, cambiando el encabezado del paquete para que contenga la siguiente información: **DIR_IP_EXTERNA:301024**.

Ahora, cuando el paquete regresa desde la red externa, el Router reconoce el prefijo (**30**) que existe en el número de puerto y con esta información puede rearmar el paquete para que este llegue a la computadora que corresponde, a la computadora **A**.

Access Point-Router WL-5404-AR

Prestaciones y Compatibilidad

El WL-5404AR está diseñado para ofrecer las máximas prestaciones inalámbricas y de router. Es capaz de tratar la información de forma rápida y eficaz. El Router está equipado con 4 bocas Switch 10/100 Mbps., con función auto MDI/MDI-X. Para aquellos que prefieran olvidarse de los cables, el WL- 5404AR integra la solución inalámbrica totalmente compatible con el estándar IEEE 802.11g y con el 802.11b. La antena es desmontable, y posibilita el intercambio con otras antenas de mayor ganancia en caso de necesidad.

Modo Nitro

Normalmente cuando dispositivos de 11 Mbps. y 54 Mbps. conviven en la misma red inalámbrica, las prestaciones de toda la red se ven reducidas ya que se adecuan a la velocidad del cliente más "lento", en este caso 11 Mbps. La familia 54 Mbps. de OvisLink está equipada con el Modo Nitro, que aumenta las prestaciones de toda la red mixta entre 11 y 54 Mbps. a la vez que minimiza las colisiones entre ambas. El resultado final: prestaciones muy superiores para toda la red inalámbrica.



Función FireWall

OvisLink ha incluido en este Router un firewall que incluye SPI (*Stateful Packet Inspection*-Inspección Completa de Paquetes), Prevención de ataques DoS (*Denial of Service*-Denegación de Servicio), filtro de paquetes VPN (*Virtual Private Network*-Red Privada Virtual). La tecnología SPI detecta situaciones donde paquetes individuales TCP/IP son válidas pero colectivamente se convierten en un ataque externo. La función de notificación de e-mail permite al Router mandar un e-mail para avisar al usuario sobre un ataque de hackers. Un filtro de contenidos y un Control de Acceso permite al administrador monitorizar y controlar la red para conseguir unas prestaciones y seguridad óptimas.

Suplemento Seguridad

Microsoft®

Elementos básicos de CRIPTOGRAFIA Parte 2

Continuamos en este artículo con el tema desarrollado en la anterior edición de NEX

Repasemos en forma breve lo que vimos en NEX5 (parte I)

Definición: la criptografía es la ciencia que nos permite proteger nuestros datos utilizando una transformación matemática de modo de transformarlos en ilegibles.

¿Qué funciones de seguridad me permite realizar la encriptación ?

Autenticación: permite a quien recibe un mensaje, estar seguro que quien lo envía es quien dice ser.
Confidencialidad: asegura que nadie leyó el mensaje desde que partió. Sólo el destinatario podrá leerlo.
Integridad: asegura que el mensaje no ha sido modificado

Para entender como lograr esto detallaremos tres conceptos básicos de criptografía:
A- Algoritmos hash en un sentido
B-Encriptación con llaves (keys, claves) simétricas: se utiliza una llave
C- Encriptación con llaves públicas y privadas: se utilizan dos llaves

En artículos posteriores desarrollaremos infraestructuras que se construyen sobre éstos. Ejemplos: firma digital o cómo haríamos para intercambiar una llave secreta. Otro ejemplo fundamental es la llamada Public Key Infrastructure (Infraestructura de llave pública) (PKI) que nos detalla las directivas, los estándares y el software que regulan o manipulan los certificados, y las llaves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica.

Hash

Un hash, también denominado valor hash o síntesis del mensaje, es un tipo de transformación de datos. Un hash es la conversión de determinados datos de cualquier tamaño, en un número de longitud fija no reversible, mediante la aplicación a los datos de una función matemática unidireccional denominada algoritmo hash. La longitud del valor hash resultante puede ser tan grande que las posibilidades de encontrar dos datos determinados que tengan el mismo valor hash son mínimas.

Funciones comunes de hash en un sentido

Las dos funciones hash siguientes son las más comunes:
MD5: es un algoritmo hash diseñado por Ron Rivest que produce un valor hash de 128 bits.
SHA-1: produce un valor hash de 160 bits. SHA-1 es un conocido algoritmo hash de un sentido utilizado para crear firmas digitales.

(parte II)

Encriptación con llaves simétricas :una sola llave.

La encriptación con llaves simétricas, es también denominada encriptación con llaves compartidas (shared keys) o criptografía de llave secreta (secret key). Se utiliza una única llave que posen tanto el remitente como el destinatario. La única llave que es usada tanto para (encriptar como desencriptar) se llama llave secreta (pero es también conocida como llave simétrica o llave de sesión). La encriptación con llaves simétricas es un método eficiente para el cifrado de grandes cantidades de datos.

Existen muchos algoritmos para la encriptación con llaves simétricas, pero todos tienen el mismo objetivo: la transformación reversible de texto sin formato (datos sin encriptar, también denominado texto no encriptado) en texto encriptado.

El texto encriptado con una llave secreta es ininteligible para quien no tenga la llave para descifrarlo. Como la criptografía de claves simétricas utiliza la misma llave tanto para la encriptación como para desencriptar, la seguridad de este proceso depende de la posibilidad de que una persona no autorizada consiga la clave simétrica. Esta es la razón por la que también se denomina criptografía de clave secreta. Quienes deseen comunicarse mediante criptografía de claves simétricas deben encontrar algún mecanismo para intercambiar de forma segura la clave antes de intercambiar datos encriptados.

El criterio principal para valorar la calidad de un algoritmo simétrico es el tamaño de su llave. Cuanto mayor sea el tamaño de la llave, habrá que probar más combinaciones de diferentes llaves para encontrar la correcta que desencripte los datos. Cuantas más claves sean necesarias, más difícil será romper el algoritmo. Con un buen algoritmo criptográfico y un tamaño adecuado de clave, es imposible, desde un punto de vista informático, que alguien invierta el proceso de transformación y obtenga el texto sin formato del texto encriptado en una cantidad de tiempo razonable.

Encriptación con llave pública: dos llaves (una pública y otra privada).

En la encriptación de llave pública (public key encription) se utilizan dos llaves: una pública y una privada, que se encuentran relacionadas matemáticamente. Para diferenciarlo del cifrado de claves simétricas, en ocasiones el cifrado de claves públicas también se denomina encriptación con llaves asimétricas.

En la encriptación de llaves públicas, la llave pública puede intercambiarse libremente entre las partes o publicarse en un repositorio público. Sin embargo, la llave privada será privada a quien cree el par (público/privado). Los datos encriptados con la llave pública sólo pueden descifrarse con la llave privada. Los datos cifrados con la llave privada sólo pueden descifrarse con la llave pública.

Al igual que la criptografía de llaves simétricas, la criptografía de llave pública también tiene diversos tipos de algoritmos. Sin embargo, el diseño de los algoritmos de llave simétrica y de llave pública es diferente.

Puede sustituir un algoritmo simétrico por otro simétrico dentro de un programa sin cambios o con cambios mínimos, ya que ambos algoritmos funcionan de la misma manera. Por otro lado, los algoritmos de llave pública que no son iguales funcionan de manera muy diferente y, por tanto, no se pueden intercambiar.

Los algoritmos de llave pública son ecuaciones matemáticas complejas en las que se utilizan cifras muy altas. Su principal inconveniente es que proporcionan formas relativamente lentas de criptografía.

En la práctica, se utilizan generalmente sólo en situaciones críticas, como en el intercambio de una llave simétrica entre entidades o para la firma de un hash de un mensaje. El uso de otras formas de criptografía, como la criptografía de llaves simétricas, junto con la criptografía de llaves públicas optimiza el rendimiento.

La encriptación por llaves públicas proporciona un método eficiente para enviar a otra persona la llave secreta que se utilizó cuando se realizó una operación de encriptación simétrico sobre una gran cantidad de datos. También puede combinar la encriptación con llaves públicas con algoritmos hash para producir una firma digital.

Algoritmos típicos de claves públicas

Los tres algoritmos siguientes de llaves públicas son los que se utilizan con más frecuencia:
RSA: para las firmas digitales y los intercambios de llaves. Hoy en día, los algoritmos criptográficos Rivest-Shamir-Adleman (RSA) son los algoritmos de llave pública más utilizados, especialmente para los datos que se envían a través de Internet. El algoritmo toma su nombre de sus tres inventores: Ron Rivest, Adi Shamir y Leonard Adleman.

La seguridad del algoritmo RSA se basa en la dificultad (en términos de velocidad y tiempo de procesamiento) de comparación de números altos. El algoritmo RSA es único entre los algoritmos de llaves públicas utilizados habitualmente ya que puede realizar operaciones tanto de firma digital como de intercambio de llaves. Los algoritmos criptográficos RSA son compatibles con Microsoft Base Cryptographic Service Provider (Microsoft Base CSP1) y con Microsoft Enhanced Cryptographic Service Provider (Microsoft Enhanced CSP2), y están integrados en numerosos productos software, incluido Microsoft Internet Explorer.

DSA: únicamente para firmas digitales. El National Institute of Standards and Technology (NIST, Instituto Nacional de Estándares y Tecnología) de Estados Unidos incorporó el Algoritmo de firma digital (DSA), inventado por la National Security Agency (NSA, Agencia de Seguridad Nacional), al Federal Information Processing Standard (FIPS, Estándar Federal para el Procesamiento de Información) para firmas digitales. El DSA obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos. Este algoritmo sólo puede utilizarse para realizar operaciones de firma digital (no para la encriptación de datos). Microsoft CSP es compatible con el algoritmo DSA.

Diffie-Hellman: únicamente para el intercambio de llaves. Diffie-Hellman, el primer algoritmo de llaves públicas, recibió el nombre de sus inventores Whitfield Diffie y Martin Hellman. Diffie-Hellman obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos en un campo finito. El algoritmo Diffie-Hellman puede utilizarse únicamente para el intercambio de llaves. Microsoft Base DSS3 y Diffie-Hellman CSP son compatibles con el algoritmo Diffie-Hellman.



Suplemento Seguridad

ACL Access Control List

Si hablamos de seguridad de la información, debemos mencionar que no existe la invulnerabilidad absoluta, pero sí ciertas formas de reducir los riesgos potenciales.

En el mundo de las redes, existen ciertos dispositivos que se encargan de que los datos enviados lleguen a destino en forma confiable. Así tenemos, por ejemplo, routers, switches, hubs, etc. Cada uno de ellos cumple una función específica. Los hubs, se encargan de distribuir el tráfico que les llega a cada una de las computadoras que tiene conectadas en sus bocas. La idea es que el tráfico entrante se envía a cada una de las computadoras que haya conectadas, llegándoles a cada una la misma información. Si una de las máquinas no requería que cierto dato le llegara, éste le llegará igual y la máquina deberá descartarlo. Si las computadoras de todo el mundo estuviesen conectadas sólo a través de hubs, sería un verdadero caos de tráfico innecesario que culminaría en que todos tendríamos acceso a todo, incluso a lo que no nos concierne. El tipo de red basada sólo en hubs puede hallarse muchas veces en *cibercafés* y en locutorios, o en redes hogareñas de más de dos computadoras.

Los switches o conmutadores, por su parte, mejoran notablemente la performance de la red al hacer que los paquetes enviados vayan sólo a aquellas máquinas que los requieren, esto es dedicando exclusivamente el ancho de banda disponible para con la máquina que lo necesite en ese instante. De esta forma no se replican datos en vano.

Los routers o enrutadores tienen como finalidad la elección de la mejor ruta para llevar el tráfico. En muchos casos además se le adicionan funciones de filtrado. Su trabajo se basa en interconectar subredes y todo esto basado en las direcciones IP (direccionamiento lógico), ya que los routers trabajan en la capa 3 del modelo de referencia OSI. Éstos se asemejan a una minicomputadora, poseen memorias, puertos de entrada y salida llamados interfaces, que permiten conectar diferentes tecnologías como son Ethernet, Token Ring y puertos seriales para la comunicación con otros routers. Se diferencian de una computadora en que no poseen un dispositivo de salida para visualizar los datos (monitor) ni uno de entrada para el ingreso de los mismos (teclado). Por lo tanto para configurarlo, se conecta a uno de sus puertos, una computadora corriendo un emulador de terminal como por ejemplo HyperTerminal en Windows, de esta manera se aprovecha el teclado y monitor. La configuración puede llevarse a cabo utilizando un web browser configurado convenientemente.

Listas de Control de Acceso

Cuando de seguridad de la información se trata, todos los recaudos que tomemos nunca resultarán en exceso, al contrario, cuantas más medidas podamos implementar siempre será ventajoso. Ante todo aclaremos que un sistema nunca contará con una seguridad absoluta del 100%, a menos que nos desconectemos físicamente de Internet, cosa necesariamente imposible hoy en día si deseamos comunicación, pero a mayor cantidad de cuidados tenidos, mejor será el resultado en términos de seguridad.

Las listas de control de acceso (ACL, en inglés, por ***Access Control Lists***) son una de las implementaciones que se llevan a cabo para reducir, no eliminar, tráfico no deseado a determinados sectores de una red.

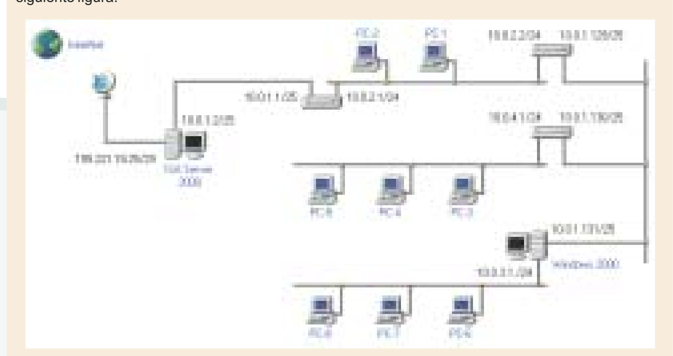
En realidad son instrucciones secuenciales que permiten definir políticas de permiso o rechazo a determinadas subredes, hosts específicos, así como también el uso de protocolos y puertos definidos.

▶▷

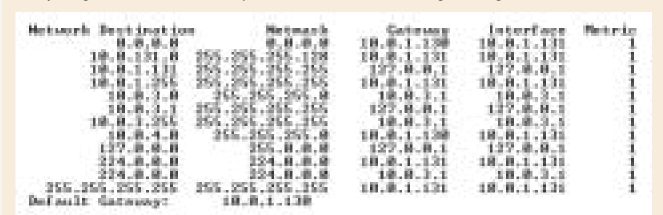
Pregunta Microsoft

Examen 070-227: Installing, Configuring and Administering MS-ISA Server 2000, Enterprise Edition

La red de su empresa consta de 3 LANs (*Local Area Network*-Red de Área Local) conectadas por medio de una MAN (*Metropolitan Area Network*-Red de Área Metropolitana). Ud. Instaló un ISA Server 2000 para proveer acceso seguro a InterNet a toda la empresa. La red esta configurada según la siguiente figura:



Usted quiere configurar las computadoras de la red como clientes SecureNAT. El router que conecta la red 10.0.3.0/24 a la MAN es un Windows 2000. Usted está revisando la configuración de las reglas de ruteo y al ingresar el comando **route print**, ve los contenidos de la siguiente figura:



Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.0.1.130	10.0.1.131	1
10.0.1.128	255.255.255.128	10.0.1.131	10.0.1.131	1
10.0.1.131	255.255.255.255	127.0.0.1	127.0.0.1	1
10.0.1.255	255.255.255.255	10.0.1.131	10.0.1.131	1
10.0.3.0	255.255.255.0	10.0.3.1	10.0.3.1	1
10.0.3.1	255.255.255.255	127.0.0.1	127.0.0.1	1
10.0.3.255	255.255.255.255	10.0.3.1	10.0.3.1	1
10.0.4.0	255.255.255.0	10.0.1.130	10.0.1.131	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	10.0.1.131	10.0.1.131	1
224.0.0.0	224.0.0.0	10.0.3.1	10.0.3.1	1
255.255.255.255	255.255.255.255	10.0.1.131	10.0.1.131	1

Default Gateway: 10.0.1.130

¿Cuál de los siguientes sets de comandos debe usar?

A. `route delete 0.0.0.0`
   `route p add 0.0.0.0 mask 0.0.0.0 10.0.1.130`

B. `route delete 0.0.0.0 mask 0.0.0.0 10.0.1.130`
   `route p add 0.0.0.0 mask 0.0.0.0 10.0.1.129`

C. `route delete 0.0.0.0`
   `route p add 0.0.0.0 10.0.1.2`

D. `route default 10.0.1.129`

Respuesta Correcta: **B**







Por ejemplo podemos autorizar o denegar a que ciertos usuarios accedan a ciertos archivos mediante HTTP o FTP. Estas instrucciones se configuran dentro del router y permiten darles características de firewall. Funcionan de manera secuencial, es decir desde la primera, en orden hasta la última. Por ello debemos meditar el orden de escritura ya que, como veremos, puede resultar que una instrucción anule, excluya o reitere a otra.

Los ejemplos que veremos están basados en routers CISCO, pero aunque difieran de otros modelos de la misma marca o de otras, podrán ser aplicadas con leves modificaciones en su configuración. Marcas como 3Com, LynkSys, D-Link, etc. sufrirán leves diferencias pero igualmente la idea podrá ser representada con bastante claridad.

Existen dos tipos de listas de acceso: *estándar* y *extendidas*.
Las primeras son las más simples y definen políticas de acceso sobre determinados hosts o subredes. Las extendidas contemplan a las estándares y abarcan también el uso de determinados grupos de hosts, protocolos, puertos, es decir son más completas.
Veamos y comentemos las estándar.

Router(config) # **access-list 1 permit 192.5.34.0 0.0.0.255**

Router(config) es el modo de configuración en el que debemos escribir nuestra lista de acceso.

La frase *access-list* y el número a continuación definen la creación de una lista de acceso, numerada como 1. Las listas de acceso estándar van numeradas del 1 al 99 y las extendidas del 100 al 199 si trabajan bajo el protocolo IP. Para los protocolos Novell IPX y AppleTalk la numeración es diferente.

Permit se refiere al hecho de autorizar el acceso del siguiente argumento. La numeración 192.5.34.0 se refiere a una dirección de subred y 0.0.0.255 se denomina máscara *wildcard*.
Esta máscara tiene como finalidad indicar cuáles hosts serán los que tendrán el acceso permitido. Vamos a mencionar que las listas de acceso deben ser asignadas a un puerto específico del router y si tendrán efecto sobre los datos entrantes o salientes del mismo. Lo veremos más adelante.

La máscara *wildcard* (comodín en inglés) funciona de la siguiente manera:

0.0.0.255 escrito en notación decimal equivaldría a 00000000.00000000.00000000.11111111 escrito en sistema binario. Se comparan octeto a octeto cada uno de bits de la dirección de subred 192.5.34.0 con los de la máscara wildcard. Visto de esta manera, se correspondería cada bit superior con el inferior.

11000000.00000101.00100010.00000000

00000000.00000000.00000000.11111111

Los bits de wildcard "0" indican que se verifican los bits de la dirección IP contra la cual se contrastan. Los bits de wildcard "1" indican que se ignoran los bits contra los cuales se comparan.

Como los bits "1" sólo afectan a la porción de host de esa dirección de subred, esto se interpreta que podrán pasar por determinada interfaz del router aquellos hosts cuya dirección IP comience con 192.5.34.xxx o sea serán desde 192.5.34.1 hasta 192.5.34.254. La dirección 192.5.34.0 no se destina al uso como host sino que queda asignada como dirección IP de subred.

Este es un mero ejemplo. Podemos denegar el acceso a uno sólo de ellos. Para ello usaríamos:

Router(config) # **access-list 2 deny host 192.5.34.18** Esto denegaría el acceso a un solo host. No hace falta indicar la máscara wildcard ya que no se trata de especificar un grupo de hosts en particular.

Si necesitáramos permitir un conjunto de hosts, no todos, deberíamos calcular cuál sería la máscara wildcard que contemplaría dicho grupo.

Por ejemplo, si deseamos dejar pasar los hosts 192.5.34.16 a 192.5.34.31 deberíamos usar una máscara wildcard 0.0.0.15, que analice solamente los últimos cuatro bits del último octeto.

16 en binario es 00010000
31 en binario es 00011111 ambos octetos difieren en los cuatro últimos bits. La máscara debe contemplar esto, por lo tanto el cuarto octeto será 00001111quedando 0.0.0.15, diferencia decimal entre 31 y 16.

Podemos ejemplificar otros casos pero excedería la intención de esta nota.

Pasemos ahora a las listas de acceso extendidas que, como dijimos, poseen funciones más completas.

Debianitas.net: Algo más que una página web

debianitas

www.debianitas.net surgió de la idea de unos entusiastas usuarios del sistema operativo Debian GNU/Linux, al ver en los foros, chats y news la inmensa masa de gente a las que se le "atraganta" la configuración y puesta apunto de su equipo. Debianitas.net intenta disponer la documentación adecuada, mediante la creación de manuales de fácil compresión, en castellano, que resuelvan las dudas más comunes para todos los usuarios. Escogimos la distribución Debian porque, a pesar de su injustificada fama de ser una distribución de "gurús", es, sin lugar a dudas, la distribución más segura, estable y potente entre las disponibles actualmente, y además, entre sus muchas ventajas (como la resolución casi-inmediata de problemas de seguridad o su sistema de mirrors de paquetes distribuidos) cabe destacar sobre todo el formato .deb, que elimina casi por completo cualquier problema de dependencias entre paquetes. Si bien Debian GNU/Linux no es una distribución muy sencilla para aquellos que no conocen este tipo de Sistemas Operativos, actualmente existen varios grupos que intentan superar cualquier tipo de barrera en los sistemas Linux, entre ellos *http://www.hispalinux.es/*, o *www.insflug.org*. Existen, además, varios weblog como *www.barrapunto.org*, o *http://bulmalug.net/* (LUG de usuarios Linux de Baleares), donde podemos estar al tanto de las últimas noticias y encontrar información de todo tipo.

Desde el proyecto debianitas intentamos aportar toda la información de nuestras propias experiencias, para facilitar y promover este sistema, disponiendo los citados manuales, así como foros, listas de correo y cualquier otra herramienta necesaria para ello. Por último decir gracias a los miles de voluntarios que con su trabajo sin ánimo de lucro, hacen que podamos disfrutar de un sistema operativo tan grande, completo, seguro y -por qué no- divertido que es Debian.



Pregunta LPI (Linux Professional Institute)

Examen 117-101-RPM

¿Qué sucede cuando rpm es lanzado de la siguiente manera?

```
rpm -Uvh file.rpm
```

A. El archivo RPM será verificado
B. Un paquete instalado se puede mejorar con la versión en el archivo, con la salida detallada
C. Un paquete instalado se puede mejorar con la versión en el archivo, con la salida detallada y marcas índice indicando el progreso
D. Un error ocurrirá porque un modo mayor no está especificado
E. Un error ocurrirá porque no se especificó ninguna opción del archivo

Respuesta correcta: **C**.
-U indica que debería ocurrir upgrade, **-h** activa marcas hash y **-v** muestra detalles de la instalación.

Examen 117-102

Desde el punto de vista del usuario, ¿Qué respuesta describe mejor la apariencia de un directorio NFS montado? Seleccione uno

A. Un nuevo dispositivo en **/dev**
B. Un nuevo volumen local tuvo acceso con una letra del volumen, por ejemplo D:
C. Un nuevo volumen local tuvo acceso con el nombre del servidor NFS
D. Parte del sistema de archivos local, tuvo acceso usando pathnames ordinarios
E. Parte del sistema de archivos de los servidores NFS, han tenido acceso usando el nombre del servidor NFS

Respuesta correcta: **D**.
Los directorios NFS montados se funden al sistema de archivo local, sin requerir una sintaxis especial para acceder.

Supongamos que queremos bloquear el acceso a la web (HTTP puerto 80) de un determinado sector de la red 192.1.1.xxx (conjunto de hosts bajo una subred). Podemos hacer lo siguiente:

Router(config) # **access-list 101 deny tcp 192.1.1.0 0.0.0.255 host 172.0.4.12 eq 80**

Como vemos, se crea una entrada dentro del ACL (101), con lo cual sabemos que se trata del tipo extendida. Estamos denegando el acceso (**deny**) al protocolo de la capa de transporte **tcp** al conjunto de hosts 192.1.1.1-254 definido por la máscara wildcard 0.0.0.255. Estos no podrán ingresar al **host 172.0.4.12**, que puede tratarse de un Web Server, utilizando el puerto 80; **eq** significa *equal* (igual). Existen otras opciones como denegar el uso de un conjunto de puertos, por ejemplo aquellos que estén por encima o por debajo de uno determinado. Esto es útil para bloquear el tráfico por puertos abiertos en vano que bien podrían significar amenazas contra la seguridad de la red, como por ejemplo el puerto 139 de NetBEUI.

Con las listas de acceso extendidas poseemos un control más exhaustivo del tráfico.

Supongamos un caso en el que nadie, por ningún motivo debe poder acceder mediante *TELNET* a ningún host de una red, además nadie tiene permisos para acceder mediante FTP. Debemos escribir una instrucción para cada caso.

Router(config) # **access-list 123 deny tcp any any eq 23**
Router(config) # **access-list 123 deny tcp any any eq 21**

(donde 23 y 21 son los puertos que usan los servicios de TELNET y FTP respectivamente.)

Notemos que no son dos listas de acceso diferentes sino dos instrucciones de una misma ACL.

La palabra **any** sirve para identificar a cualquier host origen y destino, nótese como aparece dos veces. Es una forma abreviada de representar a todos los host sin importar cuál sea. Utilizando máscaras wildcard podríamos haber escrito extensamente:

Router(config) # **access-list 123 deny 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23**
Router(config) # **access-list 123 deny 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 21**

En un comienzo dijimos que las instrucciones de una ACL se ejecutan en forma secuencial. Por lo tanto, reiteramos meditar el orden de escritura. Debemos destacar que debajo de la última condición que escribamos existe en forma implícita una orden **deny any**. Esto implica que, por defecto, se niega todo acceso salvo aquello que se haya permitido con anterioridad. Recíprocamente si son utilizadas órdenes **deny** en lugar de **permit**, debería agregarse una última línea que fuese **permit any**, ya que ésta no se encuentra implícita y, de no agregarla, cabría la posibilidad de que se niegue todo tráfico, el declarado en la lista y aquel que no lo haya sido.

Finalmente debemos asignar la lista generada a la interfaz de un router y determinar si va a filtrar el tráfico entrante o el saliente.

Deberíamos agregar la siguiente instrucción en la línea de comandos de la configuración de la interfaz determinada, por ejemplo Ethernet 0:

Router(config) # **interface E0**
Router(config-if) # **ip access-group 123 in**

El número de lista de acceso debe respetarse. Es válido para ACL estándar o extendida. Esto indica que estamos asignando las instrucciones de la lista de acceso 123 a la interfaz E0 del router. El tráfico analizado será el entrante (**in**). Si deseamos configurar el análisis de tráfico saliente, cambiamos **in** por **out**.

Como vemos, con un poco de dedicación cualquier persona podría comprometer la seguridad de una empresa si se le permite alcanzar un rack de routers. Sea por ignorancia o en forma malintencionada, podemos convertir una fortaleza en una montaña de heno. Una de las políticas de seguridad que debería de implementarse en toda empresa es justamente, evitar que el personal no idóneo acceda físicamente al sector dónde se hallan equipos comprometidos.

Leonel F. Becchio

El objetivo de las listas de control de acceso (ACL, en inglés, por Access Control Lists) son una de las implementaciones que se llevan a cabo para reducir, no eliminar, tráfico no deseado a determinados sectores de una red.

Pregunta CompTIA

Examen Security+

¿Qué tipo de IDS está diseñado para detectar archivos posiblemente modificados en una computadora que fue atacada por un Hacker?

A. NIDS
B. HIDS
C. SIV
D. LFM

Respuesta Correcta: **C**

NIDS es *Network Intrusion Detection System* (Sistema de Detección de Intrusiones a la Red)

HIDS es *Host Intrusion Detection System* (Sistema de Detección de Intrusiones a la Computadora)

SIV es *System Integrity Verifier* (Verificador de Integridad del Sistema)

LFM es *Log File Monitor* (Monitor de Archivos de Log)

Principios de E-Business



En *"Principios del e-Business"*, el fundador, presidente del Consejo y CEO de Siebel Systems, Tom Siebel, muestra cómo éstos y otros líderes de mercado aplican las tecnologías de la información y la comunicación para comprender y satisfacer mejor a sus clientes. Gracias a la tecnología actual del e-Business, las empresas pueden llevar a cabo transacciones del modo que deseen sus clientes: en cualquier parte, en cualquier momento, en cualquier idioma y moneda, y a través de cualquier canal.

Siebel asegura que en el entorno competitivo de hoy en día esa habilidad no es solamente una opción; es imprescindible para la supervivencia del negocio. La era del e-Business es en realidad la era del cliente. Su nueva fuerza le permite pasarse a la competencia con una facilidad y rapidez sin precedentes. No existe nada más decisivo para el éxito en los negocios que unas cotas altas de satisfacción del cliente.

Aunque las empresas todavía deban competir en precio, calidad de producto y distribución, estos factores no son suficientes para aventajar a la competencia. Solamente las empresas que puedan satisfacer constantemente las necesidades de sus clientes, incluso adelantarse a ellas, ganarán a batalla de la fidelidad del cliente. Y Tom Siebel sabe lo que dice. Siebel Systems es el mayor proveedor mundial de software aplicado al e-Business, la tecnología que permite muchas de las mayores y más conocidas empresas transforma rse en líderes del e-Business centrado en el cliente. Partiendo de la experiencia directa en su empresa de la implementación de sistemas de e-Business, Siebel desvela los ocho principios esenciales del e-Business y perfila un proceso directo en cinco pasos que cualquier empresa puede seguir para convertirse en un efectivo e-Business.

Ilustrado con detallados casos de estudio que ofrecen una visión desde dentro de la estrategia del e-Business en empresas como Chase, Dow Chemical, Honeywell, Quick and Reilly, y otras, "*Principios del e-Business*" es, ni más ni menos que un manifiesto para el éxito en el hipercompetitivo mercado actual.

Fuente: http://www.cuspide.com/detalle_libro.php?isbn=8475778976

SPANGLISH

Spanglish, el nuevo idioma

Increíble pero real, nuestro idioma se está llenando de expresiones idiomáticas que son verdaderas aberraciones, aunque algunos piensen que usarlas implica tener una habilidad especial, amplitud de vocabulario, y el conocimiento de ambos idiomas.

Consisten en traducciones del inglés al español que muchas veces dejan de lado cualquier norma semántica, sintáctica u ortográfica, se realizan de manera inconsciente y es un proceso cultural que cada vez gana más aceptación.

Los ejemplos más comunes son: las palabras en inglés que se escriben como se pronuncian (Ej.: Cuter, tiner, sánguche, etc.), los verbos del inglés que se conjugan con las reglas del español (Ej.: clickear, logonear, forwardear, formatear, etc), los vocablos del inglés que directamente reemplazan a palabras castellanas (Ej.: "sponsor" por auspiciante, "set" por conjunto, "blister" por envase, "shopping" por mercado, etc.), uso de palabras en inglés por el desconocimiento de una en español (Ej.: doping, rating, casting, etc.), en el caso de los adolescentes que dicen "sorry" en vez de "lo lamento", o "please" en lugar de "por favor", se puede intuir que hay una preferencia del inglés sobre la lengua propia, pero la verdadera causa de este fenómeno merece un estudio más profundo.

Por un lado, usar esta mezcla lingüística favorece y agiliza la comunicación, aunque esto es verdad sólo entre aquellos que conocen ambas lenguas. Caso contrario, la dificulta e impide.

Pensemos, por ejemplo, en una persona que no tiene ningún conocimiento de inglés a quién se le dice: "*El workshop sobre marketing comienza a las 10 y el break es a las 10:45*".

La Real Academia Española últimamente ha comenzado a aceptar a aquellos vocablos cuyo uso se ha generalizado en amplias zonas del dominio hispano parlante, procurando en lo posible, adaptar los términos foráneos a las estructuras de nuestro idioma.

Por ejemplo, la palabra "whisky" se ha cambiado por "güisqui", y "standard" se ha incorporado como "estándar".
Por mi parte, espero que esta inclusión no implique la compra de un diccionario de spanglish para poder *"speakear"* esta lengua.

Si después de todo lo dicho hay todavía alguien tan irresponsable como para iniciarse en este lenguaje, no tiene más que descargarse el diccionario traductor gratuito de spanglish que encontrará en la dirección http://www.tecapro.com/spanglish.html y comenzar a practicar.



María Luján Zito





Año. 3 Nro.6

VMWare Workstation 4



Una máquina virtual es una aplicación que permite emular varias otras máquinas dentro de una misma. ¿Cómo es esto? Permite que se corran diversos sistemas operativos simultáneamente como si se tratara de máquinas independientes, pero bajo el soporte de una sola máquina física, aquella sobre la cual corra la máquina virtual.



Desde la existencia de este tipo de software se pueden correr varios sistemas operativos simultáneamente sin la necesidad de tener una máquina para cada uno de ellos. Las aplicaciones que corren desde las máquinas virtuales no se distinguen en absoluto de las instaladas en una máquina física. Por convención, usaremos el término *host* para referirnos a la máquina que servirá de soporte para correr nuestra aplicación y, el término *guest*, para referirnos al sistema operativo que instalaremos dentro de la máquina virtual. Las características de la máquina host deberán ser bastantes elevadas, sobre todo en lo que concierne a memoria ya que cada sistema operativo que corramos nos llevará una buena parte de la misma.

¿Por qué elegiríamos utilizar máquinas virtuales? Las razones son varias y trataremos de ejemplificarlas.

- Si Ud. se dedica a realizar soporte técnico telefónico bajo diferentes sistemas operativos, una máquina física corriendo diversos sistemas operativos puede resultarle ideal ya que concentraría todas las consultas derivándolas a una misma estación de trabajo sin necesidad de optar por el uso de diversas máquinas. Resultaría más costoso equiparse de diversos equipos que adquirir uno solo y correr en él la máquina virtual. Ud. seguramente se estará preguntando si en vez de eso, no le conviene particionar su disco e instalar diversos sistemas operativos en diferentes particiones. La ventaja aquí reside en el hecho de que una máquina virtual le permite correrlos en forma simultánea en diversas ventanas como si estuviera corriendo diferentes aplicaciones, con la salvedad de que serán diferentes sistemas operativos.
- Ud. podría dedicarse a la enseñanza, entrenamiento o capacitación de personal en los diversos sistemas operativos. Para eso podría correr varios sistemas operativos sin tener que reiniciar el equipo e incluso utilizar los mismos equipos para diferentes clases, cada uno con su propio sistema operativo.
- Si Ud. está dispuesto a migrar los sistemas operativos de su empresa a una versión superior o incluso a otro sistema, debería pensar seriamente en una máquina virtual. La ventaja que le proporciona es que puede seguir utilizando aplicaciones que corran en su vieja plataforma, ya que una vez producida la migración al nuevo sistema, Ud. instala una máquina virtual y sobre ella la vieja plataforma con todas sus aplicaciones.
- En un nivel inferior podría seguir utilizando hardware no compatible con nuevos sistemas operativos, ya que la máquina virtual que aloje un sistema operativo compatible con el hardware permitiría esto.
- Si usted es programador de aplicaciones podría evaluar las mismas en diferentes entornos desde un mismo equipo.

¿Cómo trabaja una máquina virtual?

Habitualmente las computadoras corren un sistema operativo por vez. Esos sistemas operativos utilizan drivers para comunicarse con el hardware instalado como teclado, mouse, controladores de disco rígido, tarjetas de red, etc. Una máquina virtual usa el hardware instalado en el equipo y lo comparte con cada uno de los sistemas operativos que corran dentro de ella. Algunos componentes de hardware son "virtualizados", es decir, emulados por software.

Estos componentes incluyen controladores de interrupciones, controladores de DMA, controladores de dispositivos IDE/ATA, de teclado, de mouse, buses, de memoria, etc. De esta manera pueden convivir diversos sistemas operativos dentro de un mismo equipo ya que gran parte del hardware es emulado por la máquina virtual para cada uno de ellos.
Lo que comparten entre todos son los dispositivos de entrada / salida como unidades de discos flexibles, de CD-ROM, CD-R y por supuesto memoria del sistema y microprocesador. Por tal motivo, cuanta más memoria tengamos más sistemas operativos podremos correr simultáneamente.
Con respecto al espacio en disco rígido, cada máquina virtual posee su propio "disco rígido", es decir un archivo designado en el disco rígido real. Este archivo parte de un tamaño establecido y crece conforme vayamos agregando aplicaciones a nuestro sistema operativo *guest*.

VMware Workstation 4
Requerimientos recomendados del sistema

- Solamente correrá en sistemas operativos de 32 bits, aquellos de 64 bits no son soportados.
  - Procesador de 500MHz mínimo, 1GB o más recomendado. Soporta multiprocesamiento.
  - Memoria de 256 MB mínima. Debe soportar el sistema operativo de la máquina host más todos los sistemas operativos guest.
  - Al menos 1GB de espacio en disco para cada máquina virtual creada.
  - Soporta discos IDE o SCSI, CD-ROM y DVD-ROM.
  - Monitor SVGA con resolución recomendada de 800 x 600.

Podemos instalar VMware Workstation 4 en los siguientes sistemas operativos:
- Windows 2003 Server Web Edition, Standard Edition, Enterprise Edition.
- Windows XP Professional Edition y Home Edition con Service Pack 1 o sin él.
- Windows 2000 Professional, Server y Advanced Server con Service Packs 1,2,3 o sin ellos.
- Windows NT Workstation 4.0 con SP 6a, Server 4.0 con SP 6a, Terminal Server Edition 4.0 con SP 6.

También existe una versión para Linux que corre sobre diversas distribuciones como SuSE, Mandrake, Red Hat con varios release del kernel. Para mayor información visite *www.vmware.com* donde podrá bajarse la guía del usuario y consultar muchas otras especificaciones). En el sitio *www.vmware.com/landing/ws4_home.html* usted podrá bajar una versión de prueba por 30 días.

Sistemas operativos soportados

Dentro de VMware Workstation 4, podremos instalar los siguientes sistemas operativos:

- MS-DOS 6.x
  - Windows 3.1, 3.11 for Workgroup, 95, 98, 98SE, Me.
  - Windows NT y sus variantes.
  - Windows 2000 y sus variantes.
  - Windows XP Professional y Home Edition.
  - Windows 2003 y sus variantes.
  - Linux en algunas de sus distribuciones como Mandrake, Turbolinux, Red Hat, SuSE.
  - FreeBSD
  - Novell Netware 5.1 y 6.
  - Otros sistemas operativos.

Bajo una plataforma Windows XP Professional hemos probado Sun Solaris 9 junto a Red Hat Linux 9 y Windows 2000 Professional y los tres corren satisfactoriamente.

La única desventaja para los sistemas operativos que no se listan es que VMware Workstation 4 no brinda soporte a través de sus VMware Tools (Ver Herramientas...). Por ejemplo, al instalar Solaris 9, Ud. encontrará la dificultad de que la resolución de vídeo no puede ajustarse a su voluntad. Para ello, existen documentos en Internet que explican cómo hacerlo en función de la experiencia de quién los escribe.

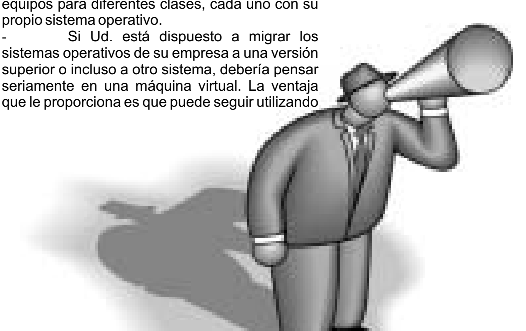


Figura nro. 1



Figura nro. 2



Creación de una máquina virtual

Vamos al menú *File>New>New Virtual Machine* y se nos desplegará un asistente que nos guiará a través del proceso de creación de la máquina virtual. (Ver Figura 1)

Luego debemos elegir *Typical* si deseamos una instalación predeterminada y *Custom* si deseamos elegir por ejemplo la cantidad de memoria asignada a dicha máquina virtual. (Ver Figura 2)

A continuación debemos elegir el sistema operativo que instalaremos dentro de la máquina virtual. (Ver Figura 3)

Luego elegimos un nombre para la máquina virtual y la ubicación donde se copiarán los archivos. (Ver Figura 4)

Aquí debemos optar entre cuatro opciones:

Use bridged networking permite conectarse a la red como si se tratan de máquinas independientes. Debemos asignarle a la máquina virtual una dirección IP diferente de la máquina física.

Use network address translation (NAT) permite que la máquina virtual utilice la dirección IP de la máquina física para conectarse a la red usando traducción de direcciones.

Use host-only networking permite que la máquina virtual se comunique solamente con la máquina física pero no con otras máquinas de una red.

Do not use a network connection inhabilita el uso de conexiones de red.

Por último *Finalizar.* (Ver Figura 5)

Presionamos *Start this virtual machine* previamente habiendo insertado el CD de instalación del sistema operativo correspondiente. Lo que sigue son los pasos de instalación del sistema operativo particular, lo cual dejaremos en manos del lector. (Ver figura 6)

Nota: Si durante la instalación del sistema operativo guest deseado por Ud. le aparece un mensaje diciéndole que el sistema debe reiniciar o que el sistema de archivos pasará a ser NTFS o algo por el estilo, NO SE ASUSTE, lo que se reiniciará será la máquina virtual, no la física, y el disco cuyo sistema de archivos deba ser modificado será el archivo.vmx que contendrá la máquina virtual creada por Ud.

Luego de la instalación completa del sistema operativo y habiendo éste booteado, es recomendable instalar VMware Tools. (Ver patilla de Herramientas...)

Leonel F. Becchio

Figura nro. 6

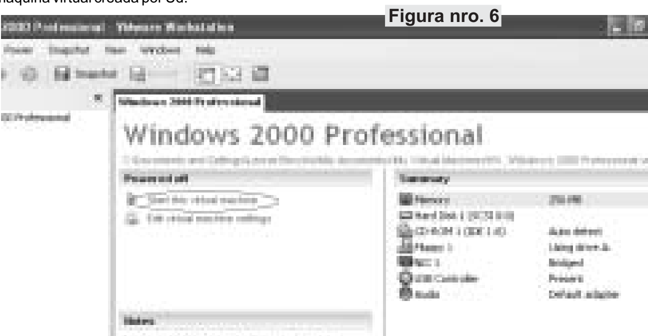


Figura nro. 3



Figura nro. 4



Figura nro. 5



Herramientas VMware

VMware Tools

No es imprescindible que debamos instalarlas pero brindan funcionalidades adicionales al sistema operativo guest una vez instalado.

Entre las funcionalidades que nos agregan encontraremos la sincronización del reloj del sistema operativo host y el guest, la función de *Cortar y Pegar* y de *Arrastrar y Soltar* entre los diversos sistemas operativos, el hecho de que podamos compartir carpetas entre sistemas. Además brinda soporte para la resolución de pantalla y el uso de mouse.

Con respecto al mouse, si nos encontramos en el escritorio del sistema operativo host y hacemos clic dentro de la ventana en la que está corriendo otro sistema operativo (guest), el control del mouse pasa a manos de este último.

Para regresar el control del mismo al sistema operativo host debemos presionar Ctrl + Alt.

Virtual PC 2004 de Microsoft

En septiembre de 2003, Microsoft adquirió la licencia para producir Virtual PC. El producto anteriormente pertenecía a la firma Connectix y en diciembre último se ha lanzado por primera vez bajo la propiedad de Microsoft, Virtual PC 2004.



Microsoft Virtual PC 2004 se puede instalar en los siguientes sistemas operativos:

- Windows 2000 Professional
- Windows XP Professional
- Windows XP Tablet PC Edition

Dentro del mismo podremos instalar los siguientes sistemas operativos:

- MS-DOS 6.22
- Windows 95
- Windows 98,98 SE
- Windows Me
- Windows 2000 Professional
- Windows NT Workstation 4.0 con Service Pack 6 o mayor.
- Windows XP Professional y Home Edition
- OS/2 Warp 4 Fixpack 15, Convenience pack 1 y 2.



En su sitio no existe especificación alguna de que Virtual PC 2004 corra sobre Linux ni que soporte el mismo, aunque esto si está indocado en Windows and .NET Magazine de Dic. 2003.

La ventaja es que Microsoft posee soporte en Argentina. Para más información visite *www.microsoft.com/windowsxp/virtualpc*. Allí podrá encontrar una versión de prueba por 45 días del producto Connectix Virtual PC for Windows, el cual es la versión anterior a Microsoft Virtual PC 2004.

Windows Server 2003

En este artículo se destacan las nuevas características introducidas por Microsoft a su nuevo sistema operativo Windows Server 2003, con respecto a sus predecesores Windows 2000 y Windows NT.

Cuatro tipos de Server

Las variantes previas al Windows Server 2003

En un principio bajo el ambiente Windows NT 4 existía únicamente una versión un poco más potente, y costosa que la estándar, llamada Enterprise Edition, que ofrecía un modelo de memoria distinto y capacidad de clustering, pero no mucho más que eso.
Ya bajo Windows 2000 el sistema básico era llamado Windows 2000 Server y el Enterprise se convirtió en Windows 2000 Advance Server. Su característica más llamativa era una nueva herramienta llamada Network Load Balancing Module (módulo de balanceo de carga de red).

Además Microsoft comenzó a desarrollar otra versión llamada Windows 2000 Datacenter Server que, como característica principal, podía soportar un cluster de hasta 8 computadoras. El problema era que estaba disponible bajo licencia OEM, y sólo los integradores de sistemas podían comprarlo y adaptarlo a su hardware particular.

Las versiones de Windows Server 2003

Microsoft introdujo un número de nuevas prestaciones con la aparición de Windows Server 2003, pero no todas están disponibles en las diferentes versiones. Los cuatro productos son:

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows Server 2003 Web Edition

Por primera vez desde 1983 Windows Server tiene un nombre, en este caso Standard Edition, el cual viene con muchas nuevas características y con otras que si bien no son nuevas no estaban presentes en las versiones básicas, como es el caso del Network Load Balancing.

Es bueno saber que con Windows Server 2003 viene un nuevo conjunto de herramientas totalmente integrables a Windows XP

La más nueva de las opciones es el Web Edition. La idea es que mediante la inclusión del servicio de Internet Information Service (IIS), pueda competir y vencer a las versiones que Apache y Sun tienen como solución de servidor web.
Es por esto que Microsoft comienza a ofrecer la versión en forma OEM quitándole algunas características que no eran necesarias para un servidor Web.

Con Server 2003, Microsoft ofrece Enterprise Edition que puede manejar clusters de cuatro computadoras y permite iniciar un servidor desde un Storage Area Network (SAN, área de almacenamiento de red), Hot-Install RAM (instalación de memoria en caliente) al igual que Datacenter, y trabajar con cuatro procesadores. Por otro lado, Datacenter Edition, soportando clusters de 8 computadoras, trae una herramienta llamada Windows Resource Manager (Administrador de recursos de Windows) la cual permite realizar la administración como podía realizarse años antes con los mainframes.

El soporte de XP se convierte en Server

Por primera vez en años Microsoft dividió a NT en dos partes, entregando por un lado NT Workstation como Windows XP, y NT Server como Windows Server 2003.
Sin embargo Windows XP es una actualización tecnológica para Windows 2000 Professional que puede considerarse poco importante e innecesaria.

La integración de XP

Windows 2000 Server trajo consigo un archivo llamado adminpak.msi que permite instalar todas las herramientas administrativas para una red en una computadora con Windows 2000 Professional. Instalando este archivo se puede realizar cualquiera de esas actividades de administración de red desde cualquier escritorio. Pero con XP la cosa cambió. Ninguna de las herramientas de administración funciona en XP bajo un entorno de red Windows 2000.

Es bueno saber que con Windows Server 2003 viene un nuevo conjunto de herramientas totalmente integrables a XP. Además dos de las más importantes características de XP como son Remote Control / Support (control / soporte remoto), y las capacidades de restricción de software ahora sí pueden ser usadas bajo el entorno de Server 2003.

Nuevos servidores gratuitos: un servidor de e-mail y un servidor de SQL "Lite"

Windows Server 2003, en cualquiera de sus versiones incluye un servidor POP3. La otra parte, el servidor SMTP, siempre ha existido, entonces entre ambas forman un completo pero sencillo servidor de correo electrónico.

Entre los inconvenientes que presenta este servidor encontramos que no hay posibilidad de usar un software antivirus en red, no hay manera de configurar que la casilla redireccione, y no se puede crear un mensaje de respuesta automática para una casilla.

La otra novedad es un nuevo motor de base de datos gratuito. Se trata de una versión reducida de SQL Server 2000 con restricciones en el acceso a la base de datos a un máximo de cinco usuarios por vez sin que se deteriore la velocidad de conexión con un tamaño máximo de la misma de 2 Gb. y sin herramientas administrativas.

Eliminación de problemas con RRAS NBT Proxy

Routing and Remote Access Service (servicio de ruteo y acceso remoto) ha sido siempre causa de grandes problemas debido a que uno de sus principales trabajos es permitir networking a través de dial-up, y este tipo de conexiones son ruidosas y poco confiables.



Novedades adicionales de trabajo en red

Compatibilidad de NAT (Network Area Translation) Traversal e IPSec

XP introdujo este concepto de NAT traversal, que permite la comunicación entre dos redes con números de IP privadas mediante el servicio Internet Connection Sharing (Conexión Compartida a Internet).

Un problema grave en cualquier sistema es la transmisión de información importante vía Internet. IPSec (en NEX1 se desarrolla un excelente articulo sobre IPsec. Ver **www.nexweb.com.ar**) (Seguridad IP) fue desarrollado para cubrir esta falla permitiendo establecer una comunicación segura a través de Internet realizando una conexión encriptada.

El problema es que hasta la aparición de Windows Server 2003 NAT e IPSec no eran compatibles. Ahora el nuevo Server trae una nueva clase de IPSec totalmente compatible con NAT Traversal. De esta forma entonces el problema de seguridad y comunicación entre redes privadas está resuelto, siempre que se tengan firewalls y routers compatibles con NAT Traversal.

Por eso Windows Server 2003 trae una característica para el servidor RRAS, llamada NBT Proxy (proxy NetBios sobre TCP/IP) que básicamente toma el Entorno de red y lo coloca como recurso completo disponible para la conexión dial-up. Por supuesto con el tiempo los usuarios deberán familiarizarse con la forma de encontrar recursos y servidores buscando en Active Directory más que navegando el Entorno de red, pero es una solución intermedia que puede facilitar la migración.

El forwarding condicional de DNS soporta DNS con AD multidominio integrado

Windows Server 2003 incorpora esta herramienta muy útil para usuarios de Active Directory con forests de más de un dominio, la cual permite que usuarios de uno de los dominios internos puedan acceder a recursos de otro dominio interno en forma directa, mediante la configuración de los servidores DNS respectivos. De esta forma se elimina uno de los inconvenientes que se presentaba en las versiones anteriores de Server al tener AD con múltiples dominios.

Mejoras en Active Directory

En Windows Server 2003 se resuelven varios problemas entre los que se puede citar la administración remota más sencilla y el incremento, insuficiente, de flexibilidad de Active Directory (AD).

Confianza forest - to - forest

Combinar un grupo de dominios AD en un forest ofrece dos beneficios principales: (1) esos dominios automáticamente confían en cada uno de los otros, y (2) los dominios comparten un set de "super" Domain Controllers (controladores de dominio) llamados Global Catalog Servers (servidores de catálogos globales), los cuales son controladores de dominio que contienen información acerca de cada dominio en el forest.
Con Windows Server 2003 se puede construir una nueva relación de confianza entre dos forest cualquiera e instantáneamente cada dominio de un forest confía en cada dominio del otro. Desafortunadamente dos forest que confían mutuamente no comparten un catálogo global. Esto significa que la confianza entre forests no deja a las aplicaciones que son dependientes de catálogos globales, ver todo el forest de confianza como un solo directorio en común. Otra limitación de la confianza de los forests es que ésta no es transitiva.

Problema de replicaciones de grupos resuelto
En Windows Server 2003 no hay límite en la cantidad de usuarios que pueden colocarse en un grupo, como si existía en Windows 2000. Además mantiene la misma característica en la estructura de Active Directory. Para obtener este beneficio se deben actualizar todos los controladores de dominio (DC) en el forest.

Novedades para oficinas remotas

Las oficinas remotas generalmente utilizan conexiones WAN que, dadas sus características, suelen ser inestables. Con Windows Server 2003 se puede hacer una copia de seguridad de la base de datos de AD del dominio, llevarla a la oficina remota, y ejecutar el asistente DCPROMO para que se pueda iniciar un nuevo controlador de dominio desde esa copia de seguridad de AD, lo cual es mejor que forzar una replicación a través de la red WAN. Luego este nuevo DC se conecta a la red y todos los DC deben actualizar los cambios que se produjeron desde el backup hasta ese momento. Esto no requiere que se actualicen los controladores de dominio.

Por otro lado AD 2003 ofrece otra característica interesante: los DC basados en Server 2003 pueden almacenar la información que necesitan de los catálogos globales. Entonces, si en algún momento se pierde la conexión de las oficinas remotas, los DC de esas oficinas tienen manera de recuperar la información necesaria y la utilizan para garantizar el inicio de sesiones en ese momento.
Los dominios pueden ser renombrados
A partir de Windows Server 2003 se pueden renombrar los dominios pero, no es una tarea sencilla. Cada DC que quiera ser renombrado debe, primero, tener Windows Server 2003 instalado y después se debe seguir un procedimiento publicado en el sitio de Microsoft en Internet de aproximadamente 60 páginas.

Active Directory puede replicar selectivamente

Esta característica elimina el inconveniente que se presenta cuando se tienen muchos controladores de dominio pero sólo algunos que actúan como servidores DNS, a través de la noción de application partition (partición de aplicación). Las particiones son subsets de AD y solamente replican a subsets de DC, ahora sólo los DC actuando como servidores DNS en una red que utiliza zonas de AD integrado van a obtener la información de DNS, y no todos.

Actualización de la administración remota

Windows 2000 tiene una herramienta muy interesante de administración remota llamada Terminal Services, pero que sólo funciona en la versión Server. A partir de la aparición de XP y Windows Server 2003 las versiones de escritorio de ambos productos incluyen una adaptación del producto de control remoto de Cytrix, que al igual que Terminal Services se basan en algo llamado Remote Desktop Protocol (protocolo de escritorio remoto, RDP). Estos productos han sido mejorados para trabajar con conexiones lentas, y además permiten dar automáticamente a la sesión de control remoto acceso a las impresoras y recursos locales.
Windows Server 2003 y XP presentan RDP en dos formas: remote desktop support (soporte de escritorio remoto) y remote assistance (asistencia remota) y en el caso de Windows 2003 se ofrece un nuevo conjunto de herramientas de control remoto en la forma de páginas Web.

Línea de comando

La consola de línea de comando permite realizar tareas similares a las realizadas a través de gran cantidad de pantallas de interfaz gráfica utilizando sólo unos cuántos caracteres, además de ejecutarse consumiendo muy poco del ancho de banda. Esto permite la creación de batch files que pueden programarse para ser ejecutados en horarios específicos y bajo determinadas condiciones. Esto es lo que la vuelve una opción muy interesante a nivel administrativo.

Mejoras en el soporte de escritorio

Hay una nueva política de grupo que dice "Ignore todos los perfiles móviles". Otra política hace a los perfiles móviles mejores para los usuarios de este tipo de equipos con Windows XP. Dependiendo de la situación en que nos encontremos, podemos elegir descargar el perfil de cuenta desde una conexión remota o no.
Windows XP y Windows Server 2003 incluyen un nuevo conjunto de políticas de grupo llamadas "políticas de restricción de software", las cuales predeterminan qué aplicaciones pueden ser utilizadas por determinados grupos de usuarios.
Por otro lado Microsoft estuvo trabajando en una herramienta para solución de conflictos de políticas llamada Group Policy Management Console (consola de administración de políticas de grupo). Esta no viene incluida en Windows Server 2003 pero pronto estará disponible en su sitio Web para ser descargada.

Seguridad ajustada

Con Windows Server 2003 se puede revertir la situación que se producía con sus antecesores, sobre todo con NT, de tener reputación de inseguros. Esto es posible porque a partir de este nuevo Server la mayoría de las opciones de seguridad que permiten cerrar accesos están cerrados de manera predeterminada a diferencia de Windows 2000 y NT en donde permanecían abiertos.

Confiabilidad

Muchas otras características de Windows Server 2003 no son realmente nuevas ya que aparecieron con Windows XP, pero nunca estuvieron disponibles para versiones Server. Por ejemplo Driver Verifier (verificador de controladores) es una herramienta para chequear los controladores de un nuevo dispositivo y otros programas a nivel del sistema. Por otro lado Driver Rollback (vuelta atrás del controlador) permite desinstalar un controlador recientemente instalado y que no haya funcionado como se esperaba.

Almacenamiento

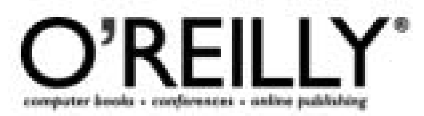
Windows XP y Windows Server 2003 trajeron muchas mejoras necesarias para NTFS: los clusters de NTFS pueden ser de cualquier tamaño, un servidor puede alojar cuantas raíces de DFS (Distributed File System) se deseen, los archivos fuera de línea pueden almacenar archivos encriptados, se pueden configurar los archivos encriptados para ser vistos por más de una persona, se puede encriptar y comprimir a la vez un archivo, y las unidades EIDE pueden trabajar en forma independiente una de la otra.

También trae algo nuevo muy interesante: "volume shadowing" que nos permite sacar copias de archivos compartidos (file shares) a diferentes horarios del día para luego recuperarlo fácil y rapidamente. (más detalles en NEX 7)

Microsoft DOS 5.0 (5.5)
Microsoft DOS 6.0 (6.2, 6.22)
Microsoft Windows 3.1 (3.11)
Microsoft Windows 95, 98 y Me
Microsoft Windows NT 3.51 Pro + Server
Microsoft Windows NT 4 Pro + Server
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Server
Microsoft Windows XP Professional
Microsoft Windows Server 2003

Y cuál crees que tenés que conocer hoy ?





O'Reilly & Associates es la fuente de información más importante de los líderes de IT. Los libros de la compañía, las conferencias, y los sitios web traen a la luz el conocimiento de este sector. Los libros de O'Reilly, conocidos por los animales en sus cubiertas, ocupan un lugar atesorado en los estantes de los desarrolladores que están construyendo la próxima generación de software. Las conferencias de O'Reilly atraen tanto a "geeks" como a líderes de negocio de pensamiento futurista para juntos darle forma a las ideas revolucionarias que dan inicio a nuevas industrias.

Descripción de la historia y la compañía

Han estado en el negocio desde 1978, originalmente como consultora de literatura técnica. En 1984, vieron las posibilidades en sistemas de código abierto y comenzaron a conservar para sí los derechos de los manuales que crearon para los vendors de Unix. En ese entonces pensaban simplemente en licenciar los libros a otros vendedores, pero para la segunda mitad de 1985, una repentina baja en el negocio de consultoría los hizo intentar publicar algo de material como libros independientes. Sus primeros títulos eran realmente más folletos que libros (un promedio de 70 páginas, los llamaron *"Nutshell Handbooks®"*, porque intentaban abordar los fundamentos), apenas lo que se necesita saber, en la menor cantidad de páginas que sea posible.
Los primeros libros fueron bien recibidos, pero el negocio de consultoría se restableció, así que continuaron publicando "en los huecos" (siempre que alguno de sus escritores tuviera tiempo muerto entre proyectos). Lo hicieron por diversión, no porque pensaran que crecería hasta ser el negocio principal en el que se ha convertido. Entonces, en enero de 1988, en una conferencia en el MIT, mostraron algunos bosquejos de los manuales Xlib que preparaban para dos de sus clientes. ¡Les fueron arrebatados! Habían planeado licenciar los libros a los vendors como documentación, pero quedó claro que había un mercado enorme para ellos como libros independientes.

Una editorial insólita

En algún punto, se dieron cuenta de que la editorial era un negocio mucho más interesante que la consultoría en documentación. Le dedicaron más y más recursos, hasta que la editorial se convirtió en la base de su negocio. Publicaron más de 300 títulos, tienen más de 300 empleados, y existen actualmente oficinas en los EE.UU., Japón, Francia, Alemania, el Reino Unido, Taiwán, y la República Popular de China. Las librerías dicen que son la editorial más consistente de libros de computación: cada libro nuevo vende, y luego continúa vendiendo.
Su entorno en el negocio de las computadoras, más que en el de la editorial tradicional, les ha dado un acercamiento muy diferente al de la mayoría de los editores de libros de computación. Muchos de sus editores son viejos programadores, administradores de sistemas, escritores técnicos, o científicos practicantes, y se espera que todos escriban por lo menos un libro propio. Al estar cerca de la industria, saben qué libros son realmente necesarios, y se aseguran de que digan a la gente lo que realmente necesitan saber. A continuación se ejemplifica con una frase usada en un catálogo hace algunos años, bajo el título de "Mitos sobre los libros de computación", que dice un poco más sobre su método de publicación: *"Usted no desea nuestros libros, usted desea la información que ellos proporcionan"*. Esta editorial realmente piensa así, por lo que ha decidido deshacerse de ciertas conjeturas que acompañan a la mayoría de los libros y documentación:

Un libro tiene que tener cierta longitud. Deben escribirse libros que concuerden con los temas que cubren, extendiéndose desde "Referencia de Bolsillo CVS" de 78 páginas, a "UNIX práctico y Seguridad en Internet", que tiene alrededor de mil páginas. **No se puede hablar mal sobre un software que funciona mal.** Absurdo. Una editorial seria es libre de expresar sus ideas. La meta es informar al lector directamente sobre los libros, aún si eso significa brindarle atajos y rodeos frente a los problemas de un software. Si el trabajo estuvo bien hecho, leer un libro debería dar la sensación de tener al lado a un usuario experimentado, pasándole datos provechosos al lector cada vez que éste se quede atascado. **Los libros no son un reemplazo para la documentación**. Se intenta escribir los libros que son tan completos como la documentación, pero tan interesantes y legibles como los libros comerciales. Una vez que usted compre un libro de esta editorial, se espera que nunca tenga que mirar la documentación otra vez, a excepción de las opciones específicas del sistema que no son estándares industriales. **Los libros no pueden mantenerse al ritmo del cambio en el mercado del software.** O´Reilly pone al día sus libros con frecuencia, a menudo realizando pequeños cambios cada vez que se reimprimen. Y mantienen los tiempos de impresión cortos a fin de tener la oportunidad de revisar cada seis meses. Uno de sus primeros libros pasó a través de diez ediciones en menos de cinco años. Muchos de los cambios son en respuesta a la comunicación con los lectores así como a cambios en el software. **Siempre hay lugar para otro libro.** Muchas editoriales compiten con ellas mismas exponiendo varios libros del mismo tema, pensando que cualquiera de ellos ganará. En O´Reilly intentan encontrar temas que ningún otro ha tocado (donde los usuarios ansían encontrar información), y hacen solamente un libro de cada tema.

O'Reilly on line

Primero, un poco de historia. Como muchos *vendors* utilizaron sus libros como documentación, tenían muchos pedidos en los ´80 para distribuir libros en varios formatos on-line (Sun AnswerBook, InfoExplorer de IBM, o LaserROM de HP). Esto era quizás una buena oportunidad de ventas, pero mantener los libros en muchos formatos diferentes parecía un negocio sin mucho interés. Se dieron cuenta de que si la publicación on line realmente tenía éxito, para ellos o para cualquier persona, necesitarían desarrollar un formato de intercambio común para los libros on line. Los editores podrían entonces permanecer en el negocio de proporcionar la información, y dejar a los *vendors* que exhiban el formato común con sus herramientas propietarias. En 1991 (junto con un grupo de vendors de pensamiento muy adelantado, incluyendo Digital Equipment Corp, Hal Computer Systems, y Silicon Graphics) fundaron el "Grupo Davenport" para explorar ediciones publicadas on line. El fruto de ese trabajo, el DocBook de DTD para SGML, ha sido adoptada como estándar de-facto de la industria por muchos de los vendors más importantes del mercado de sistema abierto (y en 1999, como SGML engendró XML, O´Reilly publicó "DocBook: La guía definitiva", escrita por un antiguo empleado de la editorial, Norm Walsh y el encargado de herramientas de producción, Lenny Muellner). Al mismo tiempo, se volvían más alertas acerca del poder de Internet. En 1993, antes de que el browser Mosaic Web fuera lanzado, descubrieron la *"World Wide Web", y* el más emocionante de los nuevos usos de Internet, la red estaba basada en una tecnología cliente-servidor hipertexto que utilizaba HTML, un dialecto de SGML, como su formato de datos.

Como resultado, su primer producto on line no era una versión electrónica de su serie Window System, sino una versión del catálogo de Internet de "The Whole Internet User´s Guide & Catalog", de Ed Krol. Comenzó como una demo, pero en poco tiempo creció hasta convertirse en un producto revolucionario ovacionado por la revista Wired como un evento histórico en la era informática. Este producto, el "Global Network Navigator", o GNN, fue el primer portal y el primer sitio web mantenido por patrocinadores. Concibieron a GNN como una interfase de información hacia Internet, un espacio cuyos artículos, noticias y boletines sobre Internet se convirtieron en la entrada a los servicios en sí. GNN fue uno de los primeros sitios web, de hecho sólo luego de una investigación profunda surgieron los 300 sitios web de la primera versión del catálogo.

Hacia finales de 1993, siglos atrás en la línea de tiempo de Internet, O´Reilly notó que la gente que estaba entusiasmada con GNN no podía conseguirlo fácilmente. Dirían: "Esto es genial. ¿Dónde lo consigo?" La respuesta es una larga historia, involucrando instrucciones para acceder a Internet, descargar software, y finalmente acostumbrarse a la web. Entonces se dieron cuenta de que necesitaban una solución de un solo paso. Trabajaron en equipo con Spry, una empresa de software con base en Seattle, para crear un producto integrado de acceso a Internet, "Internet in a Box". Éste era un software y producto de información combinados, incluyendo el software de Spry, GNN, y una versión modificada de "The Whole Internet...",

En poco tiempo, el catálogo de Internet capturó la atención de la editorial. Los proveedores de acceso a Internet crecieron como hongos, y se acercaron al juego los servicios on line. Vendieron GNN a America Online, y Spry fue vendido a CompuServe.
Continuaron su incursión en las publicaciones on line, al tiempo que la editorial y sus clientes se volvían más hacia el lado de la información tecnológica. Después de GNN, crearon "WebReview.com", un sitio enfocado a la tecnología, que le vendieron a Millar Freeman en 1999. Dale Dougherty, el fundador de GNN y WebReview.com enfocó su ingenio hacia "O´Reilly Networks", un portal para desarrolladores que se enfocan en tecnologías abiertas y emergentes. Con sitios incluyendo "XML.com", "Perl.com", y "OpenP2P.com", O´Reilly Network cubría las tecnologías más importantes con la marca registrada O´Reilly, independiente, profunda y basada en la experiencia.

Además de los desarrollos como O´Reilly en sí, también tuvieron que ver con el nacimiento de un número de empresas para explotar tecnologías. En 1996, lanzaron "MovieCritic", un sitio que se destacó por ser una de las primeras implementaciones de una depuración realizada en forma colaborativa. En la verdadera "Era de Internet", convirtieron a MovieCritic en una empresa de depuración colectiva, "LikeMinds", que más tarde se fusionó con Andromedia, que después fue comprada por Macromedia. En 1998 ayudaron a fundar "ActiveState", para lograr que Perl fuera más accesible a los usuarios de Windows. El producto ASPN de ActiveState provee herramientas, soporte y servicios para Perl, Python, y XSLT, y plug-ins de Visual Studio para estos lenguajes de forma que puedan ser usados en .NET, la nueva plataforma de Microsoft. En 1999, comenzaron "CollabNet" junto con Brian Behlendorf, cofundador de Apache Group. La misión de CollabNet fue tomar las metodologías de desarrollo colectivo de software iniciadas por proyectos de desarrollo de código abierto y hacerlos más accesibles a las corporaciones americanas.
CollabNet ha trabajado con Sun en el lanzamiento del código abierto de NetBeans, OpenOffice, y JXTA, con Oracle en Tecnología de Redes Oracle, y con muchos otros clientes corporativos que están intentando aprovechar las posibilidades que ofrece una comunidad de desarrollo colectivo.

Desde el principio, los redactores, autores, y desarrolladores de O´Reilly han sido miembros activos de las comunidades técnicas sobre cuyos trabajos se han hecho crónicas en libros y en la web.
En abril de 1998, albergaron la primer Cumbre de Código Abierto. Este evento juntó a líderes de muchas comunidades de código abierto muy importantes, incluyendo Linux, Apache, Tcl, Python, Perl y Mozilla. Fue la primera vez que los participantes se veían cara a cara. La convención generó publicidad nacional para el código abierto, llamando la atención del mundo de los negocios. Hubo otra cumbre en Marzo de 1999, que se enfocó en casos de negocios para código abierto. Y en septiembre de 2000, reunieron a líderes de compañías y organizaciones en el naciente mundo de "peer to peer". Las convenciones que hicieron han estrechado nuevos lazos entre líderes industriales, han hecho conocidas las ediciones sobre tecnología y cristalizaron las ediciones críticas sobre tecnologías emergentes.
Cuando publicaron el tan bien vendido, aunque perenne, "Programming Perl" en 1991, ayudaron a legitimizar el lenguaje a los ojos de desarrolladores corporativos. Como parte de una campaña de apoyo a la comunidad de Perl, produjeron la primera conferencia sobre "El parche de Internet" en 1997. Algunos años más tarde, agregaron conferencias sobre varias otras tecnologías de código abierto, y así nació la "Convención de Código Abierto". Se dieron cuenta de que la gente que compraba sus libros necesitaba conectarse con el otro y aprender de él, así que se metieron por completo en el negocio de las conferencias. Como su programa de publicaciones, sus conferencias se centran en la información práctica y profunda, enseñada por personas expertas (y en muchos casos, sus mismos creadores) en tecnologías de alta capacidad.

El hilo común

Para mantener los esfuerzos unidos, básicamente crearon los productos que deseaban utilizar. No importa qué forma tomen (libro, conferencia, producto on line) la idea fue que cualquier producto con el nombre O´Reilly sea útil, interesante y confiable. Y hay un montón de gente inteligente y discriminatoria en el mundo que valora esas cualidades tan profundamente como lo hacen ellos.

Más información: http://www.oreilly.com Curiosee el CV de Tim O´Reilly en: http://www.oreilly.com/oreilly/tim_bio.html

María Luján Zito